IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Agent Based Intrusion Detection System

Prof. Nisha Chaube[1], Onkar Kodape[2], Prajwal Kulkarni[3], Sahil Patil[4], Shrishail Dhole[5]
Guide, Computer Science and Engineering[1]
Students, Computer Science and Engineering[2,3,4,5]
MIT Art Design and Technology University, Pune, India
nisha.chaube@mituniversity.edu.in

Abstract: *With the growing complexity and sophistication of cyber threats, network security has become a vital aspect of any organization's cyber security efforts. Among the critical solutions, effective monitoring and analysis tools(So-In, 2009) play an invaluable role. ABIDS provides a versatile platform for real-time monitoring, alerting, and visualization of the network infrastructure. This paper attempts to demonstrate how ABIDS can serve as a basis for improved network security. Furthermore, I elaborate on ABIDS' features and abilities that make it a good choice for this purpose, such as the ability to collect the data in various ways, its compatibility with multiple protocols and devices, and its flexible alerting system. We also outline practical use-cases for ABIDS in cybersecurity operations(Ou et al., 2011), including practice recommendations on proactive threat hunting, the identification of anomalies, and timely incident responses. By incorporating ABIDS with traditional security infrastructures and solutions, organizations will be able to set up smoother and more insightful security monitoring habitats. Case studies and focused examples explain how ABIDS can help organizations enhance defence, manage risk and protect core assets against persistent cyber adversaries with adaptive capabilities(Tahri et al., 2022). We also discuss some of the deployment techniques and practices to deploy ABIDS in security-intensive environments, including the ability to scale, performance, and resource requirements. In conclusion, this paper is of the opinion that ABIDS should be strategically adopted and integrated into modern cybersecurity methods and approaches as a foundational resultant. Using ABIDS as a tool for security monitoring and analysis would strengthen the organization's defences agains6t potential cyber-attacks while ensuring the availability and integrity of their network infrastructure.*

Keywords: ABIDS